A Survey on Various Cryptographic Algorithms

Shrikant Mane
PG student, Dept of E&TC, Dr.D.Y.Patil College of Engineering, Talegaon (Ambi), Pune

Prof.R. Sathynarayana
Assistant Professor, Dept of E&TC, Dr.D.Y.Patil College of Engineering, Talegaon (Ambi), Pune

Prof.Moresh. Mukhedkar
Assistant Professor, Dept of E&TC, Dr.D.Y.Patil College of Engineering, Talegaon (Ambi), Pune

Abstract— with rapid growth of internet access users it is much easier to change the original information. Therefore many internet users worry about their document security. There is need to develop system which can protect data from hackers. Cryptography plays important role in the field of internet security. Now a day's many encryption algorithms are available . Such as DES, Blowfish, AES and MARS etc. Each one has their own benefit. User need to choose encryption algorithm according to their need. Every algorithm has their own strength and weakness. This paper present analysis of above algorithms with various parameters such as time required for encryption and decryption, encryption key size, power consumption, and most important security provided by algorithm.

Index Terms— Cryptography, Data Encryption Standard, Advanced Encryption Standard, Security, Symmetric algorithms, MARS, Blowfish.

I. INTRODUCTION

As the use of internet increasing there is a great demand for quality of service. Important aspects of encryption and decryption are privacy, authentication, identification, trust and verification. As the security demand increases the cost of cryptography algorithm increases. [1] The objectives of the cryptography are confidentiality, authentication integrity and non-repudiation. [5] Cryptography is the art of hiding information. It protects the information or data from unauthorized users. At the time of transmission original data or plaintext is encrypted i.e. Converted into unreadable form. Whenever authorized users receive this data it is converted into plaintext by performing decryption. [2] Cryptanalysis is the science of recovering the plain text of a message, without the access to the key. Brute-Force Attack tries every possible key on a piece of cipher text until an intelligible translation into plain text is obtained.

Basically there are two types of cryptosystems.

1. Symmetric cryptosystem.
2. Asymmetric cryptosystem.

Symmetric cryptosystems uses the same key for encryption and decryption. In asymmetric cryptosystem two different keys are used one for encryption and other for decryption. In asymmetric cryptosystem encryption key is public key and decryption key is private key.[5]

There are many different encryption algorithms are available, Data encryption standard (DES), 3DES, advanced encryption standard (AES), Blowfish and MARS these are secret key algorithm. [1]

II. ENCRYPTION ALGORITHMS

Data encryption standard (DES) algorithm: National bureau of standards i.e. NBS adopted DES algorithm as a new standard in 1977. It encrypts a 64 bit block into a new 64 bit block using 56 bit encryption key. The weakness of the DES is the key length. Anyone can find the key by testing different combination using known pair of plaintext and cipher text messages. [5]

3DES algorithm: 3DES algorithm is an extension of data encryption standard (DES). 3DES runs three times DES algorithm using three different keys K1, K2, K3. 3DES algorithm is too slow therefore the 128 bit Advanced encryption standard developed.[5]

Advanced encryption standard: AES adopted in 2000 by the national institute of standards and technology. AES is symmetrical algorithm and it can use three different encryption key(128 bits, 192 bits and 256 bits). AES

converts a block of 128 bits to 128 bits of cipher text. First the plaintext is converted in a 4x4 matrix i.e. state then shift row operations perform on each row. After that mix column operation and add round key operation are perform.[5]

Blowfish: it is a 64 bit symmetric block cipher. It operates in two parts 1. Key expansion part 2. Data encryption part.

The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption occurs via a 16 round feistel network.

MARS algorithm: MARS algorithm operates on block size of 128 bits with 128 bits key size. It uses shared key block ciphers. All the operations are performed on 32 bit words.

III. COMPARISON BETWEEN DES , AES, BLOWFISHAND MARS.

AES is more secure than data encryption standard. DES uses 2^{56} possible keys whereas AES uses 2^{128}, $2^{192}$and 2^{256} possible keys. DES was developed in 1977 and AES in 2000. Both the algorithm are symmetric block cipher.DES requires more encryption and decryption time as compare to AES algorithm. Triple DES provides better security than the simple DES. But it is too slow as compared to AES.[2].

In the table below shows a comparative study between DES and AES is presented in to seven factors, which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key.

TABLE I: COMPARISON BETWEEN AES AND DES [2]

FACTORS	**DES**	**AES**
Key Length	56 bits	128,192 or 256 bits
Block Size	64 bits	128,192 or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptanalysis Resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Possible Keys	256	2^{128}, $2^{192}$and 2^{256}

A good cryptosystem has to respect the avalanche effect that is stated as “small change at the input resulting in a large change at the output”[5].

Encryption time is used to calculate the throughput of an encryption scheme.

Throughput= Tp/Et

Where, Tp= Total plaintext.

Et= Encryption time [1]

IV. COMPARISON BLOWFISH AND AES

Table given below shows the comparison of encryption time between Blowfish and AES algorithm.

TABLE II: ENCRYPTION TIME COMPARISON BETWEEN BLOWFISH AND AES. [1]

Input size (kb)	Time(ms)	
	Blowfish	AES
45	40	58
76	72	87
102	90	102
500	121	134
900	220	234
1025	310	364
Average time	143.8	175.5
Throughput	18.14	15.08

Table II shows that the throughput is high for blowfish when compared to that of AES. As the throughput value is increased, the power consumption of the encryption technique is decreased. Therefore blowfish encryption algorithm consumes less power for encryption the text than that of AES [1].

Performance analysis of AES for different key size:

We consider the three different key i.e. 128 bit, 192 bit, and 256 bit keys. In case of advanced encryption standard it can be seen that higher key size leads to clear change in the battery and time consumption. It can be seen that going from 128 bits key to 192 bits causes increase in power and time consumption about 8 % and to 256 bit key causes an increase of 16 bit.

TABLE III: COMPARISON OF AES WITH DIFFERENT KEY SIZE. [1]

Input size (kb)	Time(ms)		
	AES 128	AES 192	AES 256
45	38	56	67
76	86	94	102
102	93	105	121
500	130	167	178
900	206	267	290
1025	300	301	320
Average time	142.1	165	179.6
Throughput	18.62	16.04	14.73

Above table shows that the average time required for 128 bit key size is low as compared to other two keys. Also the throughput of AES128 is greater than other two algorithms.

Speed analysis for MARS and AES algorithm:

The performance of the algorithm is measured in terms of the speed i.e. number of cycle required for the completion of the function. The speed of the algorithm can be characterized by measuring the time required for key scheduling, encryption and decryption. [4]

TABLE IV: SPEED COMPARISON BETWEEN MARS AND ADVANCED ENCRYPTION STANDARD.[4]

	Speed		Key setup	
Cipher	Encryption(cycles)	Decryption(cycles)	encryption	decryption
MARS	1600	1580	4780	5548
AES	1276	1276	17742	18886

Above table shows that the advanced encryption standard is faster than the MARS.

V. CONCLUSION

In this paper comparative study of different encryption algorithm were presented. With theoretical comparison it was concluded that the advanced encryption standard is faster than the Data encryption standard. Blowfish good for text encryption when compare to AES but AES can be used when high security is needed. Also the MARS encryption algorithm was compared with AES. In this comparison it was found that the MARS algorithm requires more cycle for encryption as well as decryption as compare to advanced encryption standard. AES 128 bit is faster and give more throughput than the AES 192 and AES 256.

REFERENCES

[1] M. Anand Kumar and Dr. S. Karthikeyan "Investigating the efficiency of blowfish and rejindael (AES) algorithms." Published online March 2012 in MECS.

[2] Shraddha Soni, Himani Agrawal,Dr.(Mrs.) Monisha Sharma "Analysis and comparison between AES and DES cryptographic algorithm" IJEIT volume 2, Issue 6, December 2012.

[3] Anurhea Dutta, Prerna Bharti, Swati Agrawal, surekha K.S "Hybrid AES-DES block Cipher" ISSN:2319-7498.

[4] Mhon H.S and A Raji Reddy "Performane analysis of AES and MARS encryption algorithms" IJCSI, col.8, Issue 4, No1,July 2011.

[5] Gabriela Moise "A survey on the usage of substitution Tables in DES and AES algorithms" Vol.LXI No.2/2009

[6] Chih- Peng Fan and Jun-Kui Hwang "FPGA implementations of high throughput aequential and fully piplined AES algorithm"

[7] Gohil Rikitaben Karsanbhai, Mary Grace Shajan "AES Algorithm for secured wireless communication"May 2011.

[8] Hoang Trang , Nguyen Van Loi "An efficient FPGA implantation of the advanced encryption standard algorithm" IEEE 2012.